REMARKS

The Office Action dated March 10, 2009, has been received and carefully noted. The above amendments to the claims, and the following remarks, are submitted as a full and complete response thereto.

By this Response, claims 1, 12, 21, 27-30, 32-34, and 48-49 have been amended to more particularly point and distinctly claim the subject matter of the present invention. No new matter has been added. Support for some of these amendments may be found in the specification, for example, at page 7, lines 8-17. Claims 8-11, 17-18, 25, 39-40, and 46 have been cancelled without prejudice or disclaimer. Accordingly, claims 1-7, 12-16, 19-24, 26-30, 32-34, 37-38, 41-45, and 47-49 are currently pending in the application of which claims 1, 12, 21, 27, 28-29, 30, 32-34, and 48-49 are independent claims.

In view of the above amendments and the following remarks, Applicants respectfully request reconsideration and timely withdrawal of the pending rejections to the claims for the reasons discussed below.

Claim Rejection - 35 U.S.C. 112

Claims 30 and 32-34 were rejected under 35 U.S.C. 112, first paragraph, as allegedly failing to comply with the written description requirement. In particular, the Office Action asserted that the limitation a "computer-readable storage medium having computer-executable components" is not included in the specification. Applicants have amended claims 30 and 32-34 to recite a "computer-readable storage medium encoded

with instructions configured to control a processor to perform a process" or a "data structure embodied on a computer-readable medium." Support for these amendments may be found in the specification, for example, at page 7, lines 18-33, which discloses client software at an user equipment (UE), and at Figure 1, which discloses an authentication server 50 allocated with an authentication server database 55. One of ordinary skill in the art would appreciate that the authentication server is typically equipped with a "computer-readable storage medium," for example, a memory, and that the authentication server database may correspond to the "computer-readable storage medium." Accordingly, Applicants respectfully submit that this rejection is moot in view of the claim amendments, and respectfully requests that this rejection be withdrawn.

Reconsideration and allowance of claims 30 and 32-34 are, thus, respectfully submitted.

Claim Rejection - 35 U.S.C. 101

Method claims 28 and 37-42 were rejected under 35 U.S.C. 101 because the claimed invention is allegedly directed to non-statutory subject matter. Specifically, the Office Action asserted that a statutory "process" under 35 U.S.C. 101 must (1) be tied to a particular machine, or (2) transform underlying subject matter (such as an article or material) to a different state or thing (*see In re Bilski*, 88 U.S.P.Q.2d 1385 (Fed. Cir. 2008)). The Office Action appears to allege that claims 28 and 37-42 are neither tied to a particular machine nor transform underlying subject matter, and thus, do not qualify as

statutory processes. Applicants have amended independent method claim 28, upon which claims 37-38 and 41-42 depend, to explicitly tie each step of the method claim to a particular machine, in particular, a processor. Applicants have also cancelled claims 39-40 without prejudice or disclaimer. Accordingly, Applicants respectfully submit that this rejection is moot in view of the claim amendments and cancellations, and respectfully requests that this rejection be withdrawn.

Reconsideration and allowance of claims 28, 37-38, and 41-42 are, thus, respectfully submitted.

Claim Rejection - 35 U.S.C. 102

Claims 1, 12, 21, 27-30, 32-34, and 48-49 were rejected under 35 U.S.C. 102(e) as allegedly being anticipated by U.S. Patent Appln. Pub. No. 2003/0176188 of O'Neill ("O'Neill"). Applicants respectfully submit that each of claims 1, 12, 21, 27-30, 32-34, and 48-49 recites subject matter that is neither disclosed nor suggested in O'Neill.

Independent claim 1, upon which claims 2-7 depend, is directed to a method including using an authentication message to signal a service selection information via a first network to an authentication server of a second network, the service selection information indicating an access point. The method also includes using the service selection information to connect to at least one service provided over the access point indicated by the service selection information. The service selection information includes at least one access point name parameter. The at least one access point parameter

includes an access point name, a username and a password. The at least one access point name parameter is encrypted in the authentication message so that the access point name can be decrypted or read by an access server, and the user name and password can only be decrypted at a network defined by the access point name.

Independent claim 12, upon which claims 13-16 and 19-20 depend, is directed to an apparatus including a processor configured to extract from a received authentication message a service selection information to select a service. The processor is configured to use the service selection information to establish a connection to services provided over an access point indicated by the service selection information. The service selection information includes at least one access point name parameter. The at least one access point name parameter includes an access point name, a username and a password. The at least one access point name parameter is encrypted in the authentication message so that the access point name can be decrypted or read by an access server, and the user name and password can only be decrypted at a network defined by the access point name.

Independent claim 21, upon which claims 22-24 and 26 depend, is directed to an apparatus including a processor configured to set in an authentication message a service selection information regarding selection of a network service. The service selection information includes at least one access point name parameter. The at least one access point name parameter includes an access point name, a username and a password. The at least one access point name parameter is encrypted in the authentication message so that

the access point name can be decrypted or read by an access server, and the user name and password can only be decrypted at a network defined by the access point name.

Independent claim 27 is directed to a system including a terminal device configured to provide access to a network service, the terminal device configured to set in an authentication message a service selection information regarding selection of the network service. The system also includes an authentication server device connected to a second network, the authentication server device configured to provide an authentication mechanism, the authentication server device configured to extract from a received authentication message the service selection information to select the service, and to use the service selection information to establish a connection to services provided over an access point indicated by the service selection information. The service selection information includes at least one access point name parameter. The at least one access point name parameter includes an access point name, a username and a password. The at least one access point name parameter is encrypted in the authentication message so that the access point name can be decrypted or read by an access server, and the user name and password can only be decrypted at a network defined by the access point name.

Independent claim 28, upon which claims 37-38 and 41-42 depend, is directed to a method including extracting, by a processor, from a received authentication message a service selection information to select a service. The method also includes using, by the processor, the service selection information to establish a connection to services provided over an access point indicated by the service selection information. The service selection

information includes at least one access point name parameter. The at least one access point name parameter includes an access point name, a username and a password. The at least one access point name parameter is encrypted in the authentication message so that the access point name can be decrypted or read by an access server, and the user name and password can only be decrypted at a network defined by the access point name.

Independent claim 29, upon which claims 43-47 depend, is directed to a method including setting in an authentication message a service selection information regarding selection of a network service at a terminal device. The service selection information includes at least one access point name parameter. The at least one access point name parameter includes an access point name, a username and a password. The at least one access point name parameter is encrypted in the authentication message so that the access point name can be decrypted or read by an access server, and the user name and password can only be decrypted at a network defined by the access point name.

Independent claim 30 is directed to a computer-readable storage medium encoded with instructions configured to control a processor to perform a process, the process including using an authentication message to signal a service selection information via a first network to a second network. The process also includes using the service selection information to connect to services provided over an access point indicated by the service selection information. The service selection information includes at least one access point name parameter. The at least one access point name parameter includes an access point name, a username and a password. The at least one access point name parameter is

encrypted in the authentication message so that the access point name can be decrypted or read by an access server, and the user name and password can only be decrypted at a network defined by the access point name.

Independent claim 32 is directed to a data structure embodied on a computer-readable medium, the data structure including a service selection information to select a service. The service selection information includes at least one access point name parameter. The at least one access point name parameter includes an access point name, a username and a password. The at least one access point name parameter is encrypted in the authentication message so that the access point name can be decrypted or read by an access server, and the user name and password can only be decrypted at a network defined by the access point name.

Independent claim 33 is directed to a computer-readable storage medium encoded with instructions configured to control a processor to perform a process, the process including extracting from a received authentication message a service selection information to select a service. The process also including using the service selection information to establish a connection to services provided over an access point indicated by the service selection information. The service selection information includes at least one access point name parameter. The at least one access point name parameter includes an access point name, a username and a password. The at least one access point name parameter is encrypted ins aid authentication message so that the access point name can

be decrypted or read by an access server, and the user name and password can only be decrypted at a network defined by the access point name.

Independent claim 34 is directed to a computer-readable storage medium encoded with instructions configured to control a processor to perform a process, the process including setting in an authentication message a service selection information regarding selection of a network service. The service selection information includes at least one access point name parameter. The at least one access point name parameter includes an access point name, a username and a password. The at least one access point name parameter is encrypted in the authentication message so that the access point name can be decrypted or read by an access server, and the user name and password can only be decrypted at a network defined by the access point name.

Independent claim 48 is directed to an apparatus including extracting means for extracting from a received authentication message a service selection information to select a service. The apparatus also includes controlling means for using the service selection information to establish a connection to services provided over an access point indicated by the service selection information. The service selection information includes at least one access point name parameter. The at least one access point name parameter includes an access point name, a username and a password. The at least one access point name parameter is encrypted in the authentication message so that the access point name can be decrypted or read by an access server, and the user name and password can only be decrypted at a network defined by the access point name.

Independent claim 49 is directed to an apparatus including setting means for setting in an authentication message a service selection information regarding selection of a network service. The apparatus also includes sending means for sending the authentication message. The service selection information includes at least one access point name parameter. The at least one access point name parameter includes an access point name, a username and a password. The at least one access point name parameter is encrypted in the authentication message so that the access point name can be decrypted or read by an access server, and the user name and password can only be decrypted at a network defined by the access point name.

Applicants respectfully submit that O'Neill fails to disclose or suggest all of the features of any of the presently pending claims.

O'Neill describes a way to extend Mobile IP Authentication Authorization and Accounting (AAA) signaling to enable a node to request from a network operator combinations of home and local service capabilities (when roaming) in an efficient and scalable manner. It also enables the home and foreign service providers to constrain and account for actual services provided based on a combination of the foreign and home operator policy (*see* O'Neill at Abstract).

However, O'Neill fails to disclose or suggest, at least, "wherein said at least one access point name parameter is encrypted in said authentication message so that said access point name can be decrypted or read by an access server, and the user name and password can only be decrypted at a network defined by the access point name," as

recited in claim 1 and similarly recited in the other independent claims. The Office Action acknowledged that O'Neill does not disclose or suggest some of these features, and cited U.S. Patent Appln. Pub. No. 2003/0146464 of Buddhikot et al. ("Buddhikot") to remedy the deficiencies of O'Neill with respect to some of these features (*see* Office Action at page 22, line 12, to page 23, line 2). Specifically, the Office Action asserted that some of these features are disclosed by Buddhikot at paragraphs 24 and 31. In the cited portion, Buddhikot refers to a home network that generates a security key to be used to encrypt/decrypt communications between a mobile node (MN) and an Access Point (AP) of a foreign network (*see also* Buddhikot at Figure 2). The MN and the foreign network have the security key, which can be used to encrypt and decrypt the communications between the MN and the AP (*see* Buddhikot at paragraphs 24 and 31). Buddhikot also refers to the foreign network including a foreign server coupled to the AP (*see* Buddhikot at paragraph 18).

However, Buddhikot fails to disclose or suggest that the communications between the MN and the AP are encrypted so that an access point name can be decrypted or read by the foreign server, and an user name and a password can only be decrypted at a network defined by the access point name. Accordingly, Buddhikot does not disclose or suggest, at least, "wherein said at least one access point name parameter is encrypted in said authentication message so that said access point name can be decrypted or read by an access server, and the user name and password can only be decrypted at a network defined by the access point name," as recited in claim 1 and similarly recited in the other

independent claims. In particular, Buddhikot fails to disclose or suggest that only a portion of the communications between the MN and the AP can be decrypted by the foreign server, and another portion of the communications can only be decrypted at a network defined by an access point name. In contrast, Buddhikot refers to the entirety of the communications between the MN and the AP being able to be decrypted by the MN and the foreign network, as discussed above. Thus, Buddhikot cannot achieve an advantage of the claimed invention: to make it not possible to access an user name and a password while transferred via a first network (*i.e.,* the foreign network of Buddhikot) (*see* Specification at page 7, lines 12-16).

For at least the reasons discussed above, Applicants respectfully submit that the combination of O'Neill and Buddhikot fails to disclose or suggest all of the elements of independent claims 1, 12, 21, 27-30, 32-34, and 48-49. Accordingly, Applicants respectfully request that the rejection of independent claims 1, 12, 21, 27-30, 32-34, and 48-49 be withdrawn.

Claim Rejections - 35 U.S.C. 103

Claims 2-7, 13-16, 22-24, 26, 37-38, 43-45, and 47 were rejected under 35 U.S.C. 103(a) as allegedly being unpatentable over O'Neill in view of U.S. Patent Appln. Pub. No. 2003/0139180 of McIntosh et al. ("McIntosh"). The Office Action acknowledged that O'Neill fails to disclose or suggest all of the features of claims 2-7, 13-16, 22-24, 26, 37-38, 43-45, and 47, and cited McIntosh to remedy the deficiencies of O'Neill with

respect to these rejected claims. Applicants respectfully submit that each of claims 2-7, 13-16, 22-24, 26, 37-38, 43-45, and 47 recites subject matter that is neither disclosed nor suggested in the combination of O'Neill and McIntosh.

In order for this rejection to be sustainable, the combination of O'Neill and McIntosh must teach all the recitations of independent claims 1, 12, 21, and 28-29. Accordingly, the arguments presented above supporting the patentability of independent claims 1, 12, 21, and 28-29 over the combination of O'Neill and Buddhikot are incorporated herein to support the patentability of dependent claims 2-7, 13-16, 22-24, 26, 37-38, 43-45, and 47. Therefore, it is respectfully requested that dependent claims 2-7, 13-16, 22-24, 26, 37-38, 43-45, and 47 be allowed. McIntosh fails to cure the deficiencies of the combination of O'Neill and Buddhikot.

McIntosh describes a communication system and a method for coupling a wireless local area network to a public network to enable communication between User Equipment terminals associated with the WLAN and the public network. The public network can include a GSM and/or a 3G-network. The WLAN can include a HiperLAN, HiperMAN, or 802.11 network. Preferably, the communication is voice communication, and the system is configured to enable the UEs to access supplementary services provided by the public network (*see* McIntosh at Abstract).

However, McIntosh fails to cure the deficiencies of the combination of O'Neill and Buddhikot. Similarly to the combination of O'Neill and Buddhikot, McIntosh fails to disclose or suggest, at least, "wherein said at least one access point name parameter is

encrypted in said authentication message so that said access point name can be decrypted or read by an access server, and the user name and password can only be decrypted at a network defined by the access point name," as recited in claim 1 and similarly recited in the other independent claims. McIntosh is silent as to teaching the particular features associated with the decryption of independent claims 1, 12, 21, and 28-29.

Therefore, the combination of O'Neill and McIntosh would not lead a person of ordinary skill in the art to arrive at the features of the decryption as recited in independent claims 1, 12, 21, and 28-29. Consequently, Applicants respectfully submit that independent claims 1, 12, 21, and 28-29 and their dependent claims 2-7, 13-16, 22-24, 26, 37-38, 43-45, and 47 are not obvious over the combination of O'Neill and McIntosh. Accordingly, Applicants respectfully request that the rejection of claims 2-7, 13-16, 22-24, 26, 37-38, 43-45, and 47 be withdrawn.

Claims 8-9, 17, 25, 39, and 46 were rejected under 35 U.S.C. 103(a) as allegedly being unpatentable over O'Neill in view of U.S. Patent Appln. Pub. No. 2002/0107964 of Tomoike ("Tomoike"). Applicants have cancelled claims 8-9, 17, 25, 39, and 46 without prejudice or disclaimer. Accordingly, Applicants respectfully submit that this rejection is moot in view of the claim cancellations, and respectfully request that this rejection be withdrawn.

Claims 10-11, 18, 20, 40, and 42 were rejected under 35 U.S.C. 103(a) as allegedly being unpatentable over O'Neill in view of Tomoike and further in view of Buddhikot. The Office Action acknowledged that the combination of O'Neill and

Tomoike fails to disclose or suggest all of the features of claims 10-11, 18, 20, 40, and 42, and cited Buddhikot to remedy the deficiencies of the combination of O'Neill and Tomoike with respect to these rejected claims. Applicants respectfully submit that each of claims 20 and 42 recites subject matter that is neither disclosed nor suggested in the combination of O'Neill, Tomoike, and Buddhikot. Applicants have cancelled claims 10-11, 18, and 40 without prejudice or disclaimer. Accordingly, Applicants respectfully submit that the rejection of claims 10-11, 18, and 40 is moot in view of the claim cancellations, and respectfully request that the rejection of claims 10-11, 18, and 40 be withdrawn.

In order for this rejection to be sustainable, the combination of O'Neill, Tomoike, and Buddhikot must teach all the recitations of independent claims 12 and 28. Accordingly, the arguments presented above supporting the patentability of independent claims 12 and 28 over the combination of O'Neill and Buddhikot are incorporated herein to support the patentability of dependent claims 20 and 42. Therefore, it is respectfully requested that dependent claims 20 and 42 be allowed. Buddhikot fails to cure the deficiencies of O'Neill.

Buddhikot describes a scheme for authentication, dynamic key generation and exchange provides means for authentication of mobile nodes and generation of per session, per node, encryption keys for encrypting/decrypting communications between a mobile node and an access point in wireless local area networks. The scheme utilizes the same infrastructure and authentication information for both data link layers (layer 2) and

network layers (layer 3). This scheme is particularly applicable to networks adhering to the IEEE 802 LAN family of standards (*see* Buddhikot at Abstract).

However, Buddhikot fails to cure the deficiencies of O'Neill. Similarly to O'Neill, Buddhikot fails to disclose or suggest, at least, "wherein said at least one access point name parameter is encrypted in said authentication message so that said access point name can be decrypted or read by an access server, and the user name and password can only be decrypted at a network defined by the access point name," as recited in claim 1 and similarly recited in the other independent claims. Buddhikot is silent as to teaching the particular features associated with the decryption of independent claims 12 and 28.

Therefore, the combination of O'Neill and Buddhikot would not lead a person of ordinary skill in the art to arrive at the features of the decryption as recited in independent claims 12 and 28. Consequently, Applicants respectfully submit that independent claims 12 and 28 and their dependent claims 20 and 42 are not obvious over the combination of O'Neill and McIntosh. Accordingly, Applicants respectfully request that the rejection of claims 20 and 42 be withdrawn.

Claims 19 and 41 were rejected under 35 U.S.C. 103(a) as allegedly being unpatentable over O'Neill in view of Tomoike and further in view of U.S. Patent Appln. Pub. No. 2003/0220107 of Lioy et al. ("Lioy"). The Office Action acknowledged that the combination of O'Neill and Tomoike fails to disclose or suggest all of the features of claims 19 and 41, and cited Lioy to remedy the deficiencies of O'Neill with respect to these rejected claims. Applicants respectfully submit that each of claims 19 and 41

recites subject matter that is neither disclosed nor suggested in the combination of O'Neill, Tomoike, and Lioy.

In order for this rejection to be sustainable, the combination of O'Neill, Tomoike, and Lioy must teach all the recitations of independent claims 12 and 28. Accordingly, the arguments presented above supporting the patentability of independent claims 12 and 28 over the combination of O'Neill and Buddhikot are incorporated herein to support the patentability of dependent claims 19 and 41. Therefore, it is respectfully requested that dependent claims 19 and 41 be allowed. Lioy fails to cure the deficiencies of the combination of O'Neill and Buddhikot.

Lioy describes a key update scheme for use in a mobile IP network. The update scheme may be implemented to facilitate key updates between a mobile device and a server computer that authenticates the mobile device. The techniques can facilitate key updates in a manner that accounts for potential message loss during the update routine, mobile device failure during the update routine, or other problems typically encountered in a mobile network settings (*see* Lioy at Abstract).

However, Lioy fails to cure the deficiencies of the combination of O'Neill and Buddhikot. Similarly to the combination of O'Neill and Buddhikot, Lioy fails to disclose or suggest, at least, "wherein said at least one access point name parameter is encrypted in said authentication message so that said access point name can be decrypted or read by an access server, and the user name and password can only be decrypted at a network defined by the access point name," as recited in claim 1 and similarly recited in the other

independent claims. Lioy is silent as to teaching the particular features associated with the decryption of independent claims 12 and 28.

Therefore, the combination of O'Neill, Tomoike, and Lioy would not lead a person of ordinary skill in the art to arrive at the features of the decryption as recited in independent claims 12 and 28. Consequently, Applicants respectfully submit that independent claims 12 and 28 and their dependent claims 19 and 41 are not obvious over the combination of O'Neill, Tomoike, and Lioy. Accordingly, Applicants respectfully request that the rejection of claims 19 and 41 be withdrawn.

Reconsideration and allowance of claims 2-7, 13-16, 19-20, 22-24, 26, 37-38, 41-45, and 47 are, thus, respectfully submitted.

Conclusion

For at least the reasons discussed above, Applicants respectfully submit that the cited references fail to disclose or suggest all of the elements of the claimed invention. These distinctions are more than sufficient to render the claimed invention unanticipated and unobvious. It is thus respectfully requested that all of claims 1-7, 12-16, 19-24, 26-30, 32-34, 37-38, 41-45, and 47-49 be allowed, and that this application be passed to issue.

If for any reason the Examiner determines that the application is not now in condition for allowance, it is respectfully requested that the Examiner contact, by

telephone, Applicants' undersigned representative at the indicated telephone number to arrange for an interview to expedite the disposition of this application.

In the event this paper is not being timely filed, Applicants respectfully petition for an appropriate extension of time. Any fees for such an extension together with any additional fees may be charged to Counsel's Deposit Account 50-2222.

Respectfully submitted,

Loren H. Tung
Registration No. 64,236

Customer No. 32294
SQUIRE, SANDERS & DEMPSEY LLP
14TH Floor
8000 Towers Crescent Drive
Vienna, Virginia 22182-6212
Telephone: 703-720-7800
Fax: 703-720-7802

LHT:skl